REMARKS

The present response is intended to be fully responsive to all points of rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Claims 1-60 are pending in this case. Claims 10, 30, 50 have been rejected under 35 U.S.C. § 112, second paragraph. Claims 1-60 have been rejected under 35 U.S.C. § 103(a). Independent claims 1, 21, 41 and dependent claims 10, 30, 50 have been amended. New claims 61-64 have been added.

With respect to the Examiner's 35 U.S.C. § 103(a) rejections, Applicant has reviewed the cited art and respectfully submits that the art fails to disclose or suggest the Applicant's claimed invention. Therefore, Applicant respectfully traverses and requests favorable reconsideration.

Response to Drawing Objections

The Examiner objected to the drawings under 37 CFR 1.84(p)(5) because they include a reference number not mentioned in the description. The specification has been amended to add the reference character 98 in the description. Applicant submits that the drawings now satisfy the requirements of 37 CFR 1.84(p)(5).

Response to 35 U.S.C. § 112, Second Paragraph Rejections

The Examiner rejected claims 10, 30, 50 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Amended claims 10, 30, 50 now feature language which make it clear what the subject matter is that the Applicant regards as the invention. Applicant believes that amended claims 10, 30, 50 overcome the Examiner's rejection based on § 112, second paragraph grounds. The Examiner is respectfully requested to withdraw the § 112, second paragraph rejection.

Response to 35 U.S.C. § 103(a) Rejections

The Examiner rejected claims 1-60 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,901,225 ("Ireton et al.") in view of U.S. Patent No. 6,247,168 ("Green). Applicant respectfully submits that the prior art fails to disclose or suggest at least XXX. Therefore, Applicant respectfully traverses the rejections and request favorable reconsideration.

While continuing to traverse the Examiner's rejections, Applicant, in order to expedite the prosecution, has chosen to clarify and emphasize the crucial distinctions between the present

invention and the devices of the patents cited by the Examiner. Specifically, claim 1 has been amended to include a method of securely downloading and installing patch data in a plurality of computing devices, each computing device having a processor, program memory and patch memory, the method comprising the steps of transmitting the patch data to the computing devices over a nonsecure channel in an encrypted manner utilizing a first key, receiving first encrypted patch data at a computing device and decrypting the first encrypted patch data utilizing the first key to generate clear patch data, verifying the integrity of the contents of the clear patch data; and if the verification passes, encrypting the clear patch data using a second key and storing the resultant second encrypted patch data in a data memory, retrieving the second encrypted patch data from the data memory and decrypting the second encrypted patch data using the second key to generate clear patch data and loading the clear patch data into the patch memory.

Ireton et al. teaches a system and method for performing software patches for embedded system devices in which the firmware resides in non-alterable storage of the device. An encryption mechanism is disclosed for increasing the security of the embedded system comprising the device. The patch is encrypted prior to storage in the external memory and decrypted as the patch is loaded into the device in order to recover the original bit sequence of the patch.

Green teaches a tool for programming non-volatile memory that is embedded in the form of an object in a programmable controller module to be used to transfer a firmware program to a plurality of different modules connected by a common network. The system comprises an encryption/decryption program. To update the firmware of a target module, the encryption program encrypts the serial number of the target module. The serial number is unique to the target module and distinguishes the target module from every other individual module in the entire PLC product line. The "approved" serial number of the target module is encrypted using the encryption key to generate an encrypted serial number which is then downloaded to the processor module. The encrypted serial number is decrypted using the key. The decrypted serial number downloaded with the patch is compared to the serial number of the target module. The update is performed only if there is a match.

It is submitted that the method of Ireton et al. uses a "one time pad" as a key used in the encryption mechanism. A string of random numbers is used to encrypt a message and is used only once to encrypt the software. See col. 10, lines 33-39. Further, the method does not indicate whether the key used is unique to a particular embedded system or common to many.

In contrast, the scheme of the present invention is operative to encrypt the patch a second time with the local unique key known only to the computing device. Further, this unique key is

repeatedly used for all patches received by the computing device. This feature is neither taught nor suggested by Ireton et al.

It is submitted that the system of Green uses the unique serial of the module in the encryption of the patch **before** it is downloaded to the module. In this system, the serial number of the target module must be supplied to the firmware producer which then encrypts the serial number with a key for transmission to the module. Green does not indicate whether the key used in the encryption of the serial number is shared or unique to the requesting module. Further, Green apparently **only** encrypts the serial number of the firmware and **not** the firmware itself.

In contrast, the scheme of the present invention uses a **shared key** known to a plurality of devices to encrypt the entire patch contents. The encrypted patch is then broadcast to all devices. No information unique to any particular device is used in preparing the patch for transmission to the devices as is done in Green. All devices that have knowledge of the shared key can receive and decrypt the patch. Once the patch is decrypted, a **second key** which is **unique** to the particular device and known only thereto is used to **re-encrypt** the patch for storage in local non-volatile memory. At startup or after a re-boot, the encrypted patch is decrypted using the local unique key and stored in patch data for execution by the processor in the computing device. None of these features are taught nor suggested by Green.

Applicant respectfully submits that the Examiner has failed to show that one of ordinary skill in the art would have been motivated to modify Ireton et al. in view of Green to arrive at the claimed invention because there is no suggestion made by Ireton et al. or Green to use a first shared key to encrypt the patch before transmitting it to a plurality of computing devices and on each individual device to use a second unique key to re-encrypt the patch once received and decrypted using the first shared key.

Applicants submit that the combination of Ireton et al. and Green would not result in the claimed invention. The Examiner has improperly combined Ireton et al. and Green in an attempt to arrive at the claimed invention. The combination suggested by the Examiner fails to teach or suggest all the claims limitations. The combination of Ireton et al. and Green fails to teach using a first shared key to encrypt the patch before transmitting it to a plurality of computing devices and on each individual device to using a second unique key to re-encrypt the patch once received and decrypted using the first shared key.

It is believed that amended independent claims 1, 21, 41 and new independent claims 61, 63 overcome the Examiner's § 103(a) rejection based on the Ireton et al. and Green references. Because Ireton et al. and Green do not anticipate or suggest claims 1, 21, 41, 61, 63 as discussed

above, then claims 2-20, 22-40, 42-60, 62, 64 are allowable as well. The Examiner is respectfully requested to withdraw the rejection based on § 103(a).

New Claims

New claims 61-64 have been added. Support for the new claims may be found throughout the specification and drawings as filed in this application. In particular, reference may be made to page 5, line 1 through page 42, line 9 and the Figures references therein. No new matter has been added.

Correction of Typographical Errors

Amendments haven been made to correct grammatical and usage errors in the specification. No new matter has been added to the application by these amendments.

Conclusion

In view of the above amendments and remarks, it is respectfully submitted that independent claims 1, 21, 41, 61, 63 and hence dependent claims 2-20, 22-40, 42-60, 62, 64 are now in condition for allowance. Prompt notice of allowance is respectfully solicited.

In light of the Amendments and the arguments set forth above, Applicant earnestly believes that they are entitled to a letters patent, and respectively solicit the Examiner to expedite prosecution of this patent applications to issuance. Should the Examiner have any questions, the Examiner is encouraged to telephone the undersigned.

Customer Number: 25937

Respectfully submitted,

ZARETSKY & ASSOCIATES PC

By: _____
Howard Zaretsky
Reg. No. 38,669
Attorney for Applicants

Zaretsky & Associates PC
8753 West Runion Dr
Peoria AZ 85382-6412
Tel.: 623-362-2585